PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-031956
(43)Date of publication of application : 28.01.2000

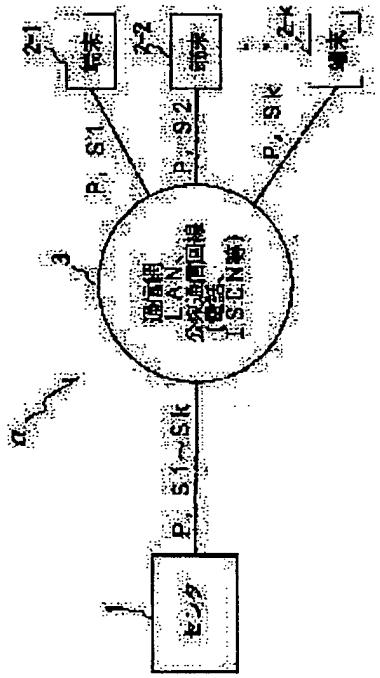
(51)Int.Cl. H04L 9/08
G09C 1/00

(21)Application number : 10-200523
(22)Date of filing : 15.07.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MINE SHINICHI
KAWAKITA TATSUJIRO
SAITO RYUICHI
NAKAHAMA KIYOSHI
YASUNAGA KENJI

(54) PERSONAL SECRET INFORMATION SHARED COMMUNICATION METHOD AND SYSTEM DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To share personal secret information at a low cost with security in common between a center and plurality of terminals without new installation of a communication line.
SOLUTION: This system is provided with a center 1 that stores common secret information P and personal secret information sets S1-Sk, discriminates legality of a request on the transmission request, encrypts the common secret information P or personal secret information sets S1-Sk and transmits the encrypted information, terminals 2-1-2-k that make transmission request of the common secret information P or the personal secret information sets S1-Sk to the center 1, decode the encrypted common secret information P or personal secret information sets S1-Sk sent from the center 1 and obtain the information, and a communication network 3 that interconnects the center 1 and the terminals 2-1-2-k.



LEGAL STATUS

[Date of request for examination] 27.10.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－31956
（P2000－31956A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｂ	５Ｋ０１３
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ｂ	
		６４０			６４０Ｂ	

審査請求　未請求　請求項の数45　ＯＬ　（全 23 頁）

(21)出願番号　特願平10－200523

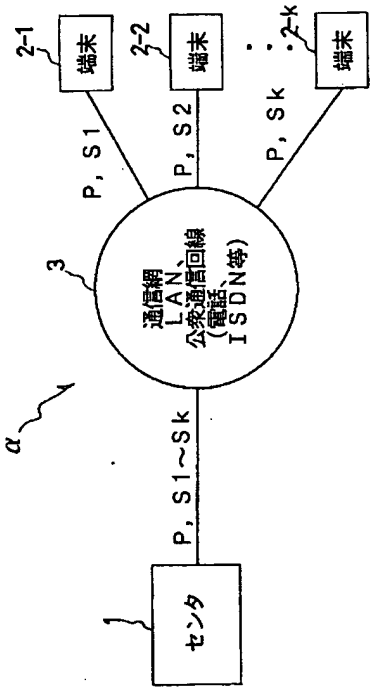
(22)出願日　平成10年７月15日(1998.7.15)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　嶺　真一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　川北　達次郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

最終頁に続く

(54)【発明の名称】　個別秘密情報共有交信方法及びシステム装置

(57)【要約】
【課題】センタと複数の端末との間で、新しく通信回線を設置することなく、安全で安価に個別秘密情報を共有することができる個別秘密情報共有交信方法及びシステム装置の提供。
【解決手段】共通秘密情報Ｐ及び個別秘密情報Ｓ１～Ｓｋを蓄積しその要求がある場合に当該要求が正常であることを判断して共通秘密情報Ｐ又は個別秘密情報Ｓ１～Ｓｋを暗号化して送信するセンタ１と、センタ１へ共通秘密情報Ｐ又は個別秘密情報Ｓ１～Ｓｋの要求を行いセンタ１から送信された暗号化された共通秘密情報Ｐ又は個別秘密情報Ｓ１～Ｓｋを復号化して得る端末２－１～２－ｋと、センタ１及び各端末２－１～２－ｋを接続する通信網３とを備える特徴。



【特許請求の範囲】
【請求項1】通信網を介して複数の端末とセンタ間においてセキュリティシステム交信を行うに当り、
予め、当該複数の端末と当該センタ相互で、当該センタに共通の共通秘密情報及び当該各端末に個有の個別秘密情報を蓄積し合い、
前記各端末から交信リクエストを前記通信網を介して受けた前記センタは、その交信リクエストが正常であるかをその都度判断した上で前記共通秘密情報又は前記個別秘密情報ともども返信レポートを含め暗号化して前記通信網を介し送信する一方、
前記センタから返信を受けた前記各端末は、送信されかつ暗号化された前記返信レポートともども復号化する前記共通秘密情報又は前記個別秘密情報を抽出消去する、
ことを特徴とする個別秘密情報共有交信方法。
【請求項2】前記交信リクエストは、
前記各端末で暗号化され、前記センタで復号化される、
ことを特徴とする請求項1に記載の個別秘密情報共有交信方法。
【請求項3】前記複数の端末は、
前記通信網を介し相互に交信可能とする、
ことを特徴とする請求項1又は2に記載の個別秘密情報共有交信方法。
【請求項4】通信網で接続された複数の端末とセンタ間においてセキュリティシステム交信を行うために、当該センタから前記複数の端末のうちの送信対象の端末へ、前記各端末で固有の秘密情報である個別秘密情報の送信を行うに当り、
前記センタにおいて、
当該センタに蓄積された前記個別秘密情報を、同じく当該センタに蓄積されて前記各端末で共通な秘密情報である前記共通秘密情報で暗号化をして暗号化個別秘密情報を作成し、当該暗号化秘密情報を含む第1のレポートを前記送信対象の端末へ前記通信網を介して送信し、
次に前記送信対象の端末において、
前記第1のレポートを受信し、当該端末に蓄積していた前記共通秘密情報で復号化をして前記個別秘密情報を取出し、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成し、当該第1のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記共通秘密情報を消去する、
ことを特徴とする個別秘密情報共有交信方法。
【請求項5】前記個別秘密情報の送信は、
その前に、前記送信対象の端末から前記センタへ前記個別秘密情報の要求を行い、その際、
前記送信対象の端末において、
当該端末に蓄積されて前記センタが前記各端末を識別可能な情報である端末情報を、同じく当該端末に蓄積された前記共通秘密情報で暗号化をしたものにより第1の署名情報を作成し、当該第1の署名情報を含むメッセージである第1のリクエストを前記通信網を介して送信し、
次に前記センタにおいて、
前記第1のリクエストを受信し前記第1の署名情報を取出し、当該センタに蓄積された前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報を取出し当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、当該第1の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第1のレポートの送信指示を行う、
ことを特徴とする請求項4に記載の個別秘密情報共有交信方法。
【請求項6】前記個別秘密情報の要求は、
前記第1の署名情報の作成に際し、
前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を、前記共通秘密情報で暗号化をして前記第1の署名情報の作成をし、
前記第1のレポートの送信指示に際し、
前記第1のリクエストを受信し第1の署名情報を取出し、前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報及び前記第1の署名識別子を取出し、当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、また取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成し、前記第1の認証結果が正常で、前記第1の確認結果が未使用の場合に行う、
ことを特徴とする請求項5に記載の個別秘密情報共有交信方法。
【請求項7】前記第1の署名情報の作成は、
前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化をしたものに、当該端末情報及び当該第1の署名識別子を付加して行い、
前記第1の認証結果の正当性の認証は、
前記端末情報及び前記第1の署名識別子を前記共通秘密情報で暗号化をしたものを復号化した復号化端末情報及び復号化第1の署名識別子と、付加された前記端末情報及び前記第1の署名識別子とを比較して、一致する場合に正常であると認証する、
ことを特徴とする請求項6に記載の個別秘密情報共有交信方法。
【請求項8】前記個別秘密情報の送信は、
その後に、前記センタから前記送信対象の端末へ前記共通秘密情報の要求を行い、その際、
前記センタにおいて、
当該センタに蓄積された前記共通秘密情報を、同じく当該センタに蓄積された前記個別秘密情報で暗号化をして暗号化共通秘密情報を作成し、当該暗号化共通秘密情報を含む第2のレポートを送信対象の前記端末へ前記通信網を介して送信し、

次に前記送信対象の端末において、
前記第２のレポートを受信し、当該端末に蓄積していた前記個別秘密情報で復号化をして前記共通秘密情報を取出し、当該共通秘密情報の受信が正常完了したか否かを示す結果である第２のレポート受信結果を作成し、当該第２のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記個別秘密情報を消去する、
ことを特徴とする請求項４、５、６又は７に記載の個別秘密情報共有交信方法。
【請求項９】前記共通秘密情報の送信は、
その前に、前記送信対象の端末から前記センタへ前記共通秘密情報の要求を行い、その際、
前記送信対象の端末において、
当該端末に蓄積された前記端末情報を、同じく当該端末に蓄積された前記個別秘密情報で暗号化をしたものにより第２の署名情報を作成し、当該第２の署名情報を含むメッセージである第２のリクエストを前記通信網を介して送信し、
次に前記センタにおいて、
前記第２のリクエストを受信し前記第２の署名情報を取出し、当該センタに蓄積された前記個別秘密情報で復号化をして前記第２の署名情報に含まれる前記端末情報を取出し当該第２の署名情報の正当性を認証した結果である第１の認証結果を作成し、当該第２の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第２のレポートの送信指示を行う、
ことを特徴とする請求項８に記載の個別秘密情報共有交信方法。
【請求項１０】前記共通秘密情報の要求は、
前記第２の署名情報の作成に際し、
前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を、前記個別秘密情報で暗号化をして前記第２の署名情報の作成をし、
前記第２のレポートの送信指示に際し、
前記第２のリクエストを受信し前記第２の署名情報を取出し、前記個別秘密情報で復号化をして前記第２の署名情報に含まれる前記端末情報及び前記第２の署名識別子を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成し、また取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成し、前記第２の認証結果が正常で、前記第２の確認結果が未使用の場合に行う、
ことを特徴とする請求項９に記載の個別秘密情報共有交信方法。
【請求項１１】前記第２の署名情報の作成は、
前記端末情報及び前記第２の署名識別子を前記個別秘密情報で暗号化をしたものに、当該端末情報及び当該第２の署名識別子を付加して行い、
前記第２の認証結果の正当性の認証は、
前記端末情報及び前記第２の署名識別子を前記共通秘密情報で暗号化をしたものを復号化した復号化端末情報及び復号化第２の署名識別子と、付加された前記端末情報及び前記第２の署名識別子とを比較して、一致する場合に正常であると認証する、
ことを特徴とする請求項１０に記載の個別秘密情報共有交信方法。
【請求項１２】前記暗号化は、
既知平文攻撃に十分な耐性のある暗号化関数を用いて行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０又は１１に記載の個別秘密情報共有交信方法。
【請求項１３】前記端末情報は、
前記各端末で重複しないものであり、
前記各端末が接続されている前記通信網におけるアドレス及び前記各端末で連続な連続番号を含める、
ことを特徴とする請求項５、６、７、８、９、１０、１１又は１２に記載の個別秘密情報共有交信方法。
【請求項１４】前記第１の署名識別子は、
前記第１の署名情報を作成する度にカウントアップする番号及び乱数を含める、
ことを特徴とする請求項６、７、８、９、１０、１１、１２又は１３に記載のに記載の個別秘密情報共有交信方法。
【請求項１５】前記第２の署名識別子は、
前記第２の署名情報を作成する度にカウントアップする番号及び乱数を含める、
ことを特徴とする請求項１０、１１、１２、１３又は１４に記載の個別秘密情報共有交信方法。
【請求項１６】前記個別秘密情報は、
前記各端末間で固有の秘密情報である端末間秘密情報を含む、
ことを特徴とする請求項３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載の個別秘密情報共有交信方法。
【請求項１７】前記個別秘密情報は、
変更可能なものであり、
時間関数及び設定自在なパラメータである世代識別子の関数を含める、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４、１５又は１６に記載の個別秘密情報共有交信方法。
【請求項１８】前記共通秘密情報は、
変更可能なものであり、
時間関数及び設定自在なパラメータである世代識別子の関数を含める、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４、１５、１６又

は１７に記載の個別秘密情報共有交信方法。
【請求項１９】前記個別秘密情報及び前記共通秘密情報は、
それぞれ、
前記暗号化を行う場合には、暗号鍵を含み、
前記認証を行う場合には、ユーザ名及びパスワード等を含み、
前記セキュリティ通信時に使用する前記通信網中の通信回線及び前記センタ及び前記各端末のポートを特定する場合には、当該通信回線及び当該ポートの情報を含む、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４、１５、１６、１７又は１８に記載の個別秘密情報共有交信方法。
【請求項２０】前記通信網は、
ＬＡＮや、電話及びＩＳＤＮを含む公衆通信回線のうちの少なくとも１つからなる、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４、１５、１６、１７、１８又は１９に記載の個別秘密情報共有交信方法。
【請求項２１】前記送信は、
前記通信網が公衆通信回線である場合に、
最初に、送信側から受信側へ発呼動作を行い、回線接続が完了した後の確保された通信チャネル上で行う、
ことを特徴とする請求項２０に記載の個別秘密情報共有交信方法。
【請求項２２】通信網に接続された複数の端末と、当該複数の各端末と前記通信網を介して接続し当該各端末で固有の秘密情報である個別秘密情報を共有するセンタとを有する個別秘密情報システム装置であって、
前記センタは、
前記各端末で共通に用いる秘密情報である共通秘密情報を蓄積する共通秘密情報センタ蓄積手段と、
前記全端末の前記個別秘密情報を蓄積する個別秘密情報センタ蓄積手段と、
前記個別秘密情報の前記各端末への送信指示を行う個別秘密情報送信指示手段と、
当該個別秘密情報送信指示手段からの送信指示に従い、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報で暗号化する暗号化個別秘密情報を含むメッセージである第１のレポートを作成し前記各端末に前記通信網を介して送信する第１のレポート作成送信手段とを有する、
ことを特徴とする個別秘密情報共有交信システム装置。
【請求項２３】前記各端末は、
前記共通秘密情報を蓄積する共通秘密情報端末蓄積手段と、
前記センタから送信される前記第１のレポートを受信し当該第１のレポートに含まれる前記暗号化個別秘密情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報で復号化し前記個別秘密情報を取出すとともに、当該個別秘密情報の受信が正常完了したか否かを示す結果である第１のレポート受信結果を作成する第１のレポート受信解析手段と、
当該第１のレポート受信解析手段で取出された前記個別秘密情報を蓄積する個別秘密情報端末蓄積手段と、
前記第１のレポート受信解析手段で作成された前記第１のレポート受信結果が正常を意味する場合に、前記共通秘密情報端末蓄積手段で蓄積している前記共通秘密情報を消去する共通秘密情報消去手段とを有する、
ことを特徴とする請求項２２に記載の個別秘密情報共有交信システム装置。
【請求項２４】前記各端末は、
前記センタで前記各端末それぞれを識別可能とする情報である端末情報を蓄積する端末情報蓄積手段と、
当該端末情報蓄積手段に蓄積された当該端末情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報とを用いて暗号化をして第１の署名情報を作成する第１の署名情報作成手段と、
前記センタに対して前記個別秘密情報を含む前記第１のレポートの送信要求を行うために、前記第１の署名情報作成手段で作成された前記第１の署名情報を含むメッセージである第１のリクエストを作成し、前記センタに前記通信網を介して送信する第１のリクエスト作成送信手段とを有する、
ことを特徴とする請求項２２又は２３に記載の個別秘密情報共有交信システム装置。
【請求項２５】前記センタは、
前記端末から送信される前記第１のリクエストを受信し、当該第１のリクエストに含まれる前記第１の署名情報を取出す第１のリクエスト受信解析手段と、
前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第１のリクエスト受信解析手段で取出された前記第１の署名情報に含まれる前記端末情報を取出し、当該第１の署名情報の正当性を認証した結果である第１の認証結果を作成する第１の署名情報認証手段とを有し、
前記第１の個別秘密情報送信指示手段は、
前記第１の署名情報認証手段で作成された前記第１の認証結果が正常の場合に、前記第１の署名情報認証手段で取出された前記第１の端末情報に示される端末への第１のレポートの送信指示を前記第１のレポート作成送信手段に対して行う機能を有する、
ことを特徴とする請求項２４に記載の個別秘密情報共有交信システム装置。
【請求項２６】前記各端末は、
前記第１の署名情報を作成する度に毎回異なる値である第１の署名識別子を作成する第１の署名識別子作成手段を有し、

前記第１の署名情報作成手段は、
前記端末情報蓄積手段に蓄積された前記端末情報と、前記第１の署名識別子作成手段で作成された前記第１の署名識別子とを、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報を用いて暗号化をして前記第１の署名情報を作成する機能を有する、
ことを特徴とする請求項２４又は２５に記載の個別秘密情報共有交信システム装置。
【請求項２７】前記第１の署名情報認証手段は、
前記共通情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第１のリクエスト情報受信解析手段で取出された前記第１の署名情報から前記端末情報及び前記第１の署名識別子を取出し前記第１の署名情報の正当性を認証した第１の認証結果を作成する機能を有し、
前記センタは、
前記第１の署名情報認証手段で取出された前記第１の署名識別子が過去に既に使用済みか否かを示す結果である第１の確認結果を作成する第１の署名識別子使用状況確認手段を有し、
前記第１の個別秘密情報送信指示手段は、
前記第１の署名情報認証手段で作成された前記第１の認証結果が正常でかつ、前記第１の署名識別子使用状況確認手段で取出された前記第１の確認結果が未使用の場合に、前記第１の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第１のレポートの送信指示を、前記第１のレポート作成送信手段に対して行う機能を有する、
ことを特徴とする請求項２６に記載の個別秘密情報共有交信システム装置。
【請求項２８】前記センタは、
前記共通秘密情報の前記各端末への送信指示を行う共通秘密情報送信指示手段と、
当該共通秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第２のレポートを作成し前記各端末に前記通信網を介して送信する第２のレポート作成送信手段とを有する、
ことを特徴とする請求項２２、２３、２４、２５、２６又は２７に記載の個別秘密情報共有交信システム装置。
【請求項２９】前記各端末は、
前記センタから送信される前記第２のレポートを受信し当該第２のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第２のレポート受信結果を作成する第２のレポート受信解析手段と、
当該第２のレポート受信解析手段で作成された前記第２のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する個別秘密情報消去手段とを有し、
前記共通秘密情報端末蓄積手段は、
前記第２のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有する、
ことを特徴とする請求項２８に記載の個別秘密情報共有交信システム装置。
【請求項３０】前記各端末は、
前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして第２の署名情報を作成する第２の署名情報作成手段と、
前記センタに対して前記共通秘密情報を含む前記第２のレポートの送信要求を行うために、前記第２の署名情報作成手段で作成された前記第２の署名情報を含むメッセージである第２のリクエストを作成し、前記センタに前記通信網を介して送信する第２のリクエスト作成送信手段とを有する、
ことを特徴とする請求項２８又は２９に記載の個別秘密情報共有交信システム装置。
【請求項３１】前記センタは、
前記端末から送信される前記第２のリクエストを受信し、当該第２のリクエストに含まれる前記署名情報を取出す第２のリクエスト受信解析手段と、
前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第２のリクエスト受信解析手段で取出された前記第２の署名情報に含まれる前記端末情報を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成する第２の署名情報認証手段とを有し、
前記共通秘密情報送信指示手段は、
前記第２の署名情報認証手段で作成された前記第２の認証結果が正常の場合に、前記第２の署名情報認証手段で取出された前記端末情報に示される端末への第２のレポートの送信指示を前記第２のレポート作成送信手段に対して行う機能を有する、
ことを特徴とする請求項３０に記載の個別秘密情報共有交信システム装置。
【請求項３２】前記各端末は、
前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を作成する第２の署名識別子作成手段を有し、
前記第２の署名情報作成手段は、
前記端末情報蓄積手段に蓄積された前記端末情報と、前記第２の署名識別子作成手段で作成された前記第２の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化して、前記第２の署名情報を作成する機能を有する、

ことを特徴とする請求項３０又は３１に記載の個別秘密情報共有交信システム装置。

【請求項３３】前記第２の署名情報認証手段は、

前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化して、前記第２のリクエスト情報受信解析手段で取出された前記第２の署名情報から前記端末情報及び前記第２の署名識別子を取出し前記第２の署名情報の正当性を認証した第２の認証結果を作成する機能を有し、

前記センタは、

前記第２の署名情報認証手段で取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成する第２の署名識別子使用状況確認手段を有し、

前記共通秘密情報送信指示手段は、

前記第２の署名情報認証手段で作成された前記第２の認証結果が正常でかつ、前記第２の署名識別子使用状況確認手段で取出された前記第２の確認結果が未使用の場合に、前記第２の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第２のレポートの送信指示を、前記第２のレポート作成送信手段に対して行う機能を有する、

ことを特徴とする請求項３２に記載の個別秘密情報共有交信システム装置。

【請求項３４】前記個別秘密情報送信指示手段は、

前記共通秘密情報の前記各端末への送信指示を行う機能も有し、

前記第１のレポート作成送信手段は、

当該個別秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第２のレポートを作成し前記各端末に前記通信網を介して送信する機能も有する、

ことを特徴とする請求項２２、２３、２４、２５、２６又は２７に記載の個別秘密情報共有交信システム装置。

【請求項３５】前記第１のレポート受信解析手段は、

前記センタから送信される前記第２のレポートを受信し当該第２のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第２のレポート受信結果を作成する機能も有し、

前記共通秘密情報消去手段は、

当該第１のレポート受信解析手段で作成された前記第２のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する機能も有し、

前記共通秘密情報端末蓄積手段は、

前記第１のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有する、

ことを特徴とする請求項３４に記載の個別秘密情報共有交信システム装置。

【請求項３６】前記第１の署名情報作成手段は、

前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報とを用いて暗号化して第２の署名情報を作成する機能も有し、

前記第１のリクエスト作成送信手段は、

前記センタに対して前記共通秘密情報を含む前記第２のレポートの送信要求を行うために、前記第２の署名情報作成手段で作成された前記第２の署名情報を含むメッセージである第２のリクエストを作成し、前記センタに前記通信網を介して送信する機能も有する、

ことを特徴とする請求項３４又は３５に記載の個別秘密情報共有交信システム装置。

【請求項３７】前記第１のリクエスト受信解析手段は、

前記端末から送信される前記第２のリクエストを受信し、当該第２のリクエストに含まれる前記署名情報を取出す機能も有し、

第１の署名情報認証手段は、

前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて、前記第２のリクエスト受信解析手段で取出された前記第２の署名情報に含まれる前記端末情報を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成する機能も有し、

前記個別秘密情報送信指示手段は、

前記第１の署名情報認証手段で作成された前記第２の認証結果が正常の場合に、前記第１の署名情報認証手段で取出された前記端末情報に示される端末への第２のレポートの送信指示を前記第１のレポート作成送信手段に対して行う機能も有する、

ことを特徴とする請求項３６に記載の個別秘密情報共有交信システム装置。

【請求項３８】前記第１の署名識別子作成手段は、

前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を作成する機能も有し、

前記第１の署名情報作成手段は、

前記端末情報蓄積手段に蓄積された前記端末情報と、前記第２の署名識別子作成手段で作成された前記第２の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして、前記第２の署名情報を作成する機能も有する、

ことを特徴とする請求項３６又は３７に記載の個別秘密情報共有交信システム装置。

【請求項３９】前記第１の署名情報認証手段は、

前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第１のリクエスト情報受信解析手段で取出された前記第２の署名情報から前記

端末情報及び前記第２の署名識別子を取出し前記第２の署名情報の正当性を認証した第２の認証結果を作成する機能も有し、
前記第１の署名識別子使用状況確認手段は、
前記第１の署名情報認証手段で取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成する第２の署名識別子使用状況確認手段を有し、
前記個別秘密情報送信指示手段は、
前記第１の署名情報認証手段で作成された前記第２の認証結果が正常でかつ、前記第１の署名識別子使用状況確認手段で取出された前記第２の確認結果が未使用の場合に、前記第１の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第２のレポートの送信指示を、前記第２のレポート作成送信手段に対して行う機能も有する、
ことを特徴とする請求項３８に記載の個別秘密情報共有交信システム装置。
【請求項４０】前記通信網は、
ＬＡＮや、電話及びＩＳＤＮを含む公衆通信回線のうちの少なくとも１つからなる、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１、３２、３３、３４、３５、３６、３７、３８又は３９に記載の個別秘密情報共有交信システム装置。
【請求項４１】前記センタは、
前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信部を有する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１、３２、３３、３４、３５、３６、３７、３８、３９又は４０に記載の個別秘密情報共有交信システム装置。
【請求項４２】前記センタとは別に、
前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信装置を設ける、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１、３２、３３、３４、３５、３６、３７、３８、３９又は４０に記載の個別秘密情報共有交信システム装置。
【請求項４３】前記センタ及び前記各端末は、
別に、前記共通秘密情報を時間関数及び設定自在なパラメータとする世代識別子の関数を入力及び蓄積する鍵注入器を設ける、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載の個別秘密情報共有交信システム装置。
【請求項４４】前記第１の署名識別子作成手段は、
前記第１の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの１つを有する、
ことを特徴とする請求項２６、２７、２８、２９、３０、３１、３２、３３、３４、３５、３６、３７、３８、３９、４０、４１、４２又は４３に記載の個別秘密情報共有交信システム装置。
【請求項４５】前記第２の署名識別子は、
前記第２の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの１つを有する、
ことを特徴とする請求項３２、３３、３８、３９、４０、４１、４２、４３又は４４に記載の個別秘密情報共有交信システム装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】センタと端末間でＬＡＮや公衆通信回線等のように予め不正アクセスやデータ不正モニタの防止機能が十分具備されていない通信回線を用いてセキュリティ通信を行う通信システムにおいて、前記通信回線を用いてセンタと各端末間で各端末毎に異なる個別秘密情報を共有可能とする個別秘密情報共有交信方法及びその実施に直接用いるシステム装置に関するものである。
【０００２】
【従来の技術】遠隔地に設置された複数の端末とセンタの間で、ＬＡＮや、電話、ＩＳＤＮ等の公衆通信回線を介して各種通信を行うシステムにおいて、その機能を安定して確実に動作させるためには、不正者によるセンタのアクセスや回線上で伝送される信号の盗聴等によるハッキング対策として、何らかのセキュリティ上の保護機能を具備しておく必要がある。
【０００３】このセキュリティ機能を実現するためには、センタと端末が自身の正当性を証明することが可能な（不正者が持ち得ない）秘密情報を共有しアクセス開始時に相互認証を行ったり、転送データの暗号化を行う方法が有効であるが、これを実現するためには、セキュリティ通信を通信を開始する前の段階で、各端末とセンタで同一の秘密情報を共有しておく必要がある。
【０００４】また、万一いずれかの端末から秘密情報が漏洩した場合に、他の端末の通信に与える影響を極力小さくするという観点からは、セキュリティ通信に用いる秘密情報は各端末毎に異なる秘密情報である個別秘密情報とすることが望ましい。
【０００５】従来は、センタと各端末の間で個別秘密情報を共有するためには、センタと端末間で安全に情報を配送できる高セキュリティ機能を具備した通信手段（例えば、信頼できる人を介して直接双方に入力したり、郵便書留等のような親展通信を用いる等）を介して、秘密情報を入出力する方法が用いられている。
【０００６】
【発明が解決しようとする課題】しかし、上記従来技術では、端末とセンタ間でＬＡＮや公衆通信回線等のよう

に予め不正アクセスやデータ不正モニタの防止機能が十分具備されていない通信回線を用いてセキュリティ通信を行おうとすると、センタと各端末間で個別秘密情報を共有するために別の高価な（かつ安全な）通信手段が必要となるため、センタに収束する端末数が多かったりその設置場所が多岐にわたっているような場合には、経済的にセキュリティ通信システムを実現することが難しいという問題点があった。

【0007】また、これを解決するために各端末に共通な秘密情報である共通秘密情報を用いて、センタと各端末間でセキュリティ通信を行おうとすると、万一上記秘密情報が漏洩した場合には、システム全体に影響が及ぶという別の問題点があった。

【0008】ここにおいて、本発明の解決すべき主要な目的は次の通りである。

【0009】本発明の第1の目的は、センタと各端末間で経済的に安価でかつ安全に個別秘密情報を共有することができる個別秘密情報共有交信方法及びシステム装置を提供せんとするものである。

【0010】本発明の第2の目的は、センタと各端末間で別の新たな通信回線を設置しなくてもよい個別秘密情報共有交信方法及びシステム装置を提供せんとするものである。

【0011】本発明の第3の目的は、万一共通秘密情報が漏洩した場合にもシステム全体に影響が及ぶことのない個別秘密情報交信共有方法及びシステム装置を提供せんとするものである。

【0012】本発明のその他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【0013】

【課題を解決するための手段】本発明は、上記課題の解決に当たり、複数の端末とセンタとを通信網で接続して当該センタにおいて個別秘密情報及び共通秘密情報を共有交信する装置の特徴を有し、前記センタにおいて前記個別秘密情報を前記共通秘密情報で暗号化して送信し、前記各端末において前記暗号化した個別秘密情報を前記共通秘密情報で復号化して前記共通秘密情報を得る方法の特徴を有する。

【0014】更に具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念に亙る新規な特徴的構成手段又は手法を採用することにより、前記目的を達成するよう為される。

【0015】即ち、本発明方法の第1の特徴は、通信網を介して複数の端末とセンタ間においてセキュリティシステム交信を行うに当り、予め、当該複数の端末と当該センタ相互で、当該センタに共通の共通秘密情報及び当該各端末に個有の個別秘密情報を蓄積し合い、前記各端末から交信リクエストを前記通信網を介して受けた前記センタは、その交信リクエストが正常であるかをその都度判断した上で前記共通秘密情報又は前記個別秘密情報ともども返信レポートを含め暗号化して前記通信網を介し送信する一方、前記センタから返信を受けた前記各端末は、送信されかつ暗号化された前記返信レポートともども復号化する前記共通秘密情報又は前記個別秘密情報を抽出消去してなる個別秘密情報共有交信方法の構成採用にある。

【0016】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における前記交信リクエストが、前記各端末で暗号化され、前記センタで復号化されてなる個別秘密情報共有交信方法の構成採用にある。

【0017】本発明方法の第3の特徴は、上記本発明方法の第1又は第2の特徴における前記複数の端末が、前記通信網を介し相互に交信可能としてなる個別秘密情報共有交信方法の構成採用にある。

【0018】本発明方法の第4の特徴は、通信網で接続された複数の端末とセンタ間においてセキュリティシステム交信を行うために、当該センタから前記複数の端末のうちの送信対象の端末へ、前記各端末で固有の秘密情報である個別秘密情報の送信を行うに当り、前記センタにおいて、当該センタに蓄積された前記個別秘密情報を、同じく当該センタに蓄積されて前記各端末で共通な秘密情報である前記共通秘密情報で暗号化をして暗号化個別秘密情報を作成し、当該暗号化秘密情報を含む第1のレポートを前記送信対象の端末へ前記通信網を介して送信し、次に前記送信対象の端末において、前記第1のレポートを受信し、当該端末に蓄積していた前記共通秘密情報で復号化をして前記個別秘密情報を取出し、当該個別秘密情報の受信が正常完了したか否かを示す結果である第1のレポート受信結果を作成し、当該第1のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記共通秘密情報を消去してなる個別秘密情報共有交信方法の構成採用にある。

【0019】本発明方法の第5の特徴は、上記本発明方法の第4の特徴における前記個別秘密情報の送信が、その前に、前記送信対象の端末から前記センタへ前記個別秘密情報の要求を行い、その際、前記送信対象の端末において、当該端末に蓄積されて前記センタが前記各端末を識別可能な情報である端末情報を、同じく当該端末に蓄積された前記共通秘密情報で暗号化をしたものにより第1の署名情報を作成し、当該第1の署名情報を含むメッセージである第1のリクエストを前記通信網を介して送信し、次に前記センタにおいて、前記第1のリクエストを受信し前記第1の署名情報を取出し、当該センタに蓄積された前記共通秘密情報で復号化をして前記第1の署名情報に含まれる前記端末情報を取出し当該第1の署名情報の正当性の認証をした結果である第1の認証結果を作成し、当該第1の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第1のレポートの送信指示を行ってなる個別秘密情

報共有交信方法の構成採用にある。

【００２０】本発明方法の第６の特徴は、上記本発明方法の第５の特徴における前記個別秘密情報の要求が、前記第１の署名情報の作成に際し、前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第１の署名情報を作成する度に毎回異なる値である第１の署名識別子を、前記共通秘密情報で暗号化をして前記第１の署名情報の作成をし、前記第１のレポートの送信指示に際し、前記第１のリクエストを受信し第１の署名情報を取出し、前記共通秘密情報で復号化をして前記第１の署名情報に含まれる前記端末情報及び前記第１の署名識別子を取出し、当該第１の署名情報の正当性の認証をした結果である第１の認証結果を作成し、また取出された前記第１の署名識別子が過去に既に使用済みか否かを示す結果である第１の確認結果を作成し、前記第１の認証結果が正常で、前記第１の確認結果が未使用の場合に行ってなる個別秘密情報共有交信方法の構成採用にある。

【００２１】本発明方法の第７の特徴は、上記本発明方法の第６の特徴における前記第１の署名情報の作成が、前記端末情報及び前記第１の署名識別子を前記共通秘密情報で暗号化をしたものに、当該端末情報及び当該第１の署名識別子を付加して行い、前記第１の認証結果の正当性の認証が、前記端末情報及び前記第１の署名識別子を前記共通秘密情報で暗号化をしたものを復号化した復号化端末情報及び復号化第１の署名識別子と、付加された前記端末情報及び前記第１の署名識別子とを比較して、一致する場合に正常であると認証してなる個別秘密情報共有交信方法の構成採用にある。

【００２２】本発明方法の第８の特徴は、上記本発明方法の第４、第５、第６又は第７の特徴における前記個別秘密情報の送信が、その後に、前記センタから前記送信対象の端末へ前記共通秘密情報の要求を行い、その際、前記センタにおいて、当該センタに蓄積された前記共通秘密情報を、同じく当該センタに蓄積された前記個別秘密情報で暗号化をして暗号化共通秘密情報を作成し、当該暗号化共通秘密情報を含む第２のレポートを送信対象の前記端末へ前記通信網を介して送信し、次に前記送信対象の端末において、前記第２のレポートを受信し、当該端末に蓄積していた前記個別秘密情報で復号化をして前記共通秘密情報を取出し、当該共通秘密情報の受信が正常完了したか否かを示す結果である第２のレポート受信結果を作成し、当該第２のレポート受信結果が正常を意味する場合に、当該端末に蓄積していた前記個別秘密情報を消去してなる個別秘密情報共有交信方法の構成採用にある。

【００２３】本発明方法の第９の特徴は、上記本発明方法の第８の特徴における前記共通秘密情報の送信が、その前に、前記送信対象の端末から前記センタへ前記共通秘密情報の要求を行いその際、前記送信対象の端末において、当該端末に蓄積された前記端末情報を、同じく当該端末に蓄積された前記個別秘密情報で暗号化をしたものにより第２の署名情報を作成し、当該第２の署名情報を含むメッセージである第２のリクエストを前記通信網を介して送信し、次に前記センタにおいて、前記第２のリクエストを受信し前記第２の署名情報を取出し、当該センタに蓄積された前記個別秘密情報で復号化をして前記第２の署名情報に含まれる前記端末情報を取出し当該第２の署名情報の正当性を認証した結果である第１の認証結果を作成し、当該第２の認証結果が正常である場合に、前記送信対象の端末である前記端末情報に示された端末へ前記第２のレポートの送信指示を行ってなる個別秘密情報共有交信方法の構成採用にある。

【００２４】本発明方法の第１０の特徴は、上記本発明方法の第９の特徴における前記共通秘密情報の要求が、前記第２の署名情報の作成に際し、前記端末情報に加えて、当該送信対象の端末に蓄積されて前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を、前記個別秘密情報で暗号化をして前記第２の署名情報の作成をし、前記第２のレポートの送信指示に際し、前記第２のリクエストを受信し前記第２の署名情報を取出し、前記個別秘密情報で復号化をして前記第２の署名情報に含まれる前記端末情報及び前記第２の署名識別子を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成し、また取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成し、前記第２の認証結果が正常で、前記第２の確認結果が未使用の場合に行ってなる個別秘密情報共有交信方法の構成採用にある。

【００２５】本発明方法の第１１の特徴は、上記本発明方法の第１０の特徴における前記第２の署名情報の作成が、前記端末情報及び前記第２の署名識別子を前記個別秘密情報で暗号化をしたものに、当該端末情報及び当該第２の署名識別子を付加して行い、前記第２の認証結果の正当性の認証が、前記端末情報及び前記第２の署名識別子を前記共通秘密情報で暗号化をしたものを復号化した復号化端末情報及び復号化第２の署名識別子と、付加された前記端末情報及び前記第２の署名識別子とを比較して、一致する場合に正常であると認証してなる個別秘密情報共有交信方法の構成採用にある。

【００２６】本発明方法の第１２の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における前記暗号化が、既知平文攻撃に十分な耐性のある暗号化関数を用いて行ってなる個別秘密情報共有交信方法の構成採用にある。

【００２７】本発明方法の第１３の特徴は、上記本発明方法の第５、第６、第７、第８、第９、第１０、第１１又は第１２の特徴における前記端末情報が、前記各端末で重複しないものであり、前記各端末が接続されている前記通信網におけるアドレス及び前記各端末で連続な連

統番号を含めてなる個別秘密情報共有交信方法の構成採用にある。

【００２８】本発明方法の第１４の特徴は、上記本発明方法の第６、第７、第８、第９、第１０、第１１、第１２又は第１３の特徴における前記第１の署名識別子が、前記第１の署名情報を作成する度にカウントアップする番号及び乱数を含めてなる個別秘密情報共有交信方法の構成採用にある。

【００２９】本発明方法の第１５の特徴は、上記本発明方法の第１０、第１１、第１２、第１３又は第１４の特徴における前記第２の署名識別子が、前記第２の署名情報を作成する度にカウントアップする番号及び乱数を含めてなる個別秘密情報共有交信方法の構成採用にある。

【００３０】本発明方法の第１６の特徴は、上記本発明方法の第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における前記個別秘密情報が、前記各端末間で固有の秘密情報である端末間秘密情報を含んでなる個別秘密情報共有交信方法の構成採用にある。

【００３１】本発明方法の第１７の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５又は第１６の特徴における前記個別秘密情報が、変更可能なものであり、時間関数及び設定自在なパラメータである世代識別子の関数を含めてなる個別秘密情報共有交信方法の構成採用にある。

【００３２】本発明方法の第１８の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６又は第１７の特徴における前記共通秘密情報が、変更可能なものであり、時間関数及び設定自在なパラメータである世代識別子の関数を含めてなる個別秘密情報共有交信方法の構成採用にある。

【００３３】本発明方法の第１９の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７又は第１８の特徴における前記個別秘密情報及び前記共通秘密情報が、それぞれ、前記暗号化を行う場合には、暗号鍵を含み、前記認証を行う場合には、ユーザ名及びパスワード等を含み、前記セキュリティ通信時に使用する前記通信網中の通信回線及び前記センタ及び前記各端末のポートを特定する場合には、当該通信回線及び当該ポートの情報を含んでなる個別秘密情報共有交信方法の構成採用にある。

【００３４】本発明方法の第２０の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７、第１８又は第１９の特徴における前記通信網が、ＬＡＮや、電話及びＩＳＤＮを含む公衆通信回線のうちの少なくとも１つからなる個別秘密情報共有交信方法の構成採用にある。

【００３５】本発明方法の第２１の特徴は、上記本発明方法の第２０の特徴における前記送信が、前記通信網が公衆通信回線である場合に、最初に、送信側から受信側へ発呼動作を行い、回線接続が完了した後の確保された通信チャネル上で行ってなる個別秘密情報共有交信方法の構成採用にある。

【００３６】本発明装置の第１の特徴は、通信網に接続された複数の端末と、当該複数の各端末と前記通信網を介して接続し当該各端末で固有の秘密情報である個別秘密情報を共有するセンタとを有する個別秘密情報システム装置であって、前記センタが、前記各端末で共通に用いる秘密情報である共通秘密情報を蓄積する共通秘密情報センタ蓄積手段と、前記全端末の前記個別秘密情報を蓄積する個別秘密情報センタ蓄積手段と、前記個別秘密情報の前記各端末への送信指示を行う個別秘密情報送信指示手段と、当該個別秘密情報送信指示手段からの送信指示に従い、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報で暗号化する暗号化個別秘密情報を含むメッセージである第１のレポートを作成し前記各端末に前記通信網を介して送信する第１のレポート作成送信手段とを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００３７】本発明装置の第２の特徴は、上記本発明装置の第１の特徴における前記各端末が、前記共通秘密情報を蓄積する共通秘密情報端末蓄積手段と、前記センタから送信される前記第１のレポートを受信し当該第１のレポートに含まれる前記暗号化個別秘密情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報で復号化し前記個別秘密情報を取出すとともに、当該個別秘密情報の受信が正常完了したか否かを示す結果である第１のレポート受信結果を作成する第１のレポート受信解析手段と、当該第１のレポート受信解析手段で取出された前記個別秘密情報を蓄積する個別秘密情報端末蓄積手段と、前記第１のレポート受信解析手段で作成された前記第１のレポート受信結果が正常を意味する場合に、前記共通秘密情報端末蓄積手段で蓄積している前記共通秘密情報を消去する共通秘密情報消去手段とを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００３８】本発明装置の第３の特徴は、上記本発明装置の第１又は第２の特徴における前記各端末が、前記センタで前記各端末それぞれを識別可能とする情報である端末情報を蓄積する端末情報蓄積手段と、当該端末情報蓄積手段に蓄積された当該端末情報を、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報とを用いて暗号化をして第１の署名情報を作成する第１の署名情報作成手段と、前記センタに対して前記個別秘密情報を含む前記第１のレポートの送信要求を行うために、前記

第1の署名情報作成手段で作成された前記第1の署名情報を含むメッセージである第1のリクエストを作成し、前記センタに前記通信網を介して送信する第1のリクエスト作成送信手段とを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0039】本発明装置の第4の特徴は、上記本発明装置の第3の特徴における前記センタが、前記端末から送信される前記第1のリクエストを受信し、当該第1のリクエストに含まれる前記第1の署名情報を取出す第1のリクエスト受信解析手段と、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト受信解析手段で取出された前記第1の署名情報に含まれる前記端末情報を取出し、当該第1の署名情報の正当性を認証した結果である第1の認証結果を作成する第1の署名情報認証手段とを有し、前記第1の個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第1の認証結果が正常の場合に、前記第1の署名情報認証手段で取出された前記第1の端末情報に示される端末への第1のレポートの送信指示を前記第1のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0040】本発明装置の第5の特徴は、上記本発明装置の第3又は第4の特徴における前記各端末が、前記第1の署名情報を作成する度に毎回異なる値である第1の署名識別子を作成する第1の署名識別子作成手段を有し、前記第1の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第1の署名識別子作成手段で作成された前記第1の署名識別子とを、前記共通秘密情報端末蓄積手段に蓄積された前記共通秘密情報を用いて暗号化をして前記第1の署名情報を作成する機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0041】本発明装置の第6の特徴は、上記本発明装置の第5の特徴における前記第1の署名情報認証手段が、前記共通情報センタ蓄積手段に蓄積された前記共通秘密情報を用いて復号化をして、前記第1のリクエスト情報受信解析手段で取出された前記第1の署名情報から前記端末情報及び前記第1の署名識別子を取出し前記第1の署名情報の正当性を認証した第1の認証結果を作成する機能を有し、前記センタが、前記第1の署名情報認証手段で取出された前記第1の署名識別子が過去に既に使用済みか否かを示す結果である第1の確認結果を作成する第1の署名識別子使用状況確認手段を有し、前記第1の個別秘密情報送信指示手段が、前記第1の署名情報認証手段で作成された前記第1の認証結果が正常でかつ、前記第1の署名識別子使用状況確認手段で取出された前記第1の確認結果が未使用の場合に、前記第1の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第1のレポートの送信指示を、前記第1のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0042】本発明装置の第7の特徴は、上記本発明装置の第1、第2、第3、第4、第5又は第6の特徴における前記センタが、前記共通秘密情報の前記各端末への送信指示を行う共通秘密情報送信指示手段と、当該共通秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第2のレポートを作成し前記各端末に前記通信網を介して送信する第2のレポート作成送信手段とを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0043】本発明装置の第8の特徴は、上記本発明装置の第7の特徴における前記各端末が、前記センタから送信される前記第2のレポートを受信し当該第2のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第2のレポート受信結果を作成する第2のレポート受信解析手段と、当該第2のレポート受信解析手段で作成された前記第2のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する個別秘密情報消去手段とを有し、前記共通秘密情報端末蓄積手段が、前記第2のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有してなる個別秘密情報共有システム装置の構成採用にある。

【0044】本発明装置の第9の特徴は、上記本発明装置の第7又は第8の特徴における前記各端末が、前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして第2の署名情報を作成する第2の署名情報作成手段と、前記センタに対して前記共通秘密情報を含む前記第2のレポートの送信要求を行うために、前記第2の署名情報作成手段で作成された前記第2の署名情報を含むメッセージである第2のリクエストを作成し、前記センタに前記通信網を介して送信する第2のリクエスト作成送信手段とを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【0045】本発明装置の第10の特徴は、上記本発明装置の第9の特徴における前記センタが、前記端末から送信される前記第2のリクエストを受信し、当該第2のリクエストに含まれる前記署名情報を取出す第2のリクエスト受信解析手段と、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第2のリクエスト受信解析手段で取出された前

記第２の署名情報に含まれる前記端末情報を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成する第２の署名情報認証手段とを有し、前記共通秘密情報送信指示手段が、前記第２の署名情報認証手段で作成された前記第２の認証結果が正常の場合に、前記第２の署名情報認証手段で取出された前記端末情報に示される端末への第２のレポートの送信指示を前記第２のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００４６】本発明装置の第１１の特徴は、上記本発明装置の第９又は第１０の特徴における前記各端末が、前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を作成する第２の署名識別子作成手段を有し、前記第２の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第２の署名識別子作成手段で作成された前記第２の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化して、前記第２の署名情報を作成する機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００４７】本発明装置の第１２の特徴は、上記本発明装置の第１１の特徴における前記第２の署名情報認証手段が、前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化して、前記第２のリクエスト情報受信解析手段で取出された前記第２の署名情報から前記端末情報及び前記第２の署名識別子を取出し前記第２の署名情報の正当性を認証した第２の認証結果を作成する機能を有し、前記センタが、前記第２の署名情報認証手段で取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成する第２の署名識別子使用状況確認手段を有し、前記共通秘密情報送信指示手段が、前記第２の署名情報認証手段で作成された前記第２の認証結果が正常でかつ、前記第２の署名識別子使用状況確認手段で取出された前記第２の確認結果が未使用の場合に、前記第２の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第２のレポートの送信指示を、前記第２のレポート作成送信手段に対して行う機能を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００４８】本発明装置の第１３の特徴は、上記本発明装置の第１、第２、第３、第４、第５又は第６の特徴における前記個別秘密情報送信指示手段が、前記共通秘密情報の前記各端末への送信指示を行う機能も有し、前記第１のレポート作成送信手段が、当該個別秘密情報送信指示手段からの送信指示に従い、前記共通秘密情報センタ蓄積手段に蓄積された前記共通秘密情報を、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報で暗号化する暗号化共通秘密情報を含むメッセージである第２のレポートを作成し前記各端末に前記通信網を介して送信する機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００４９】本発明装置の第１４の特徴は、上記本発明装置の第１３の特徴における前記第１のレポート受信解析手段が、前記センタから送信される前記第２のレポートを受信し当該第２のレポートに含まれる前記暗号化共通秘密情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報で復号化し前記共通秘密情報を取出すとともに、当該共通秘密情報の受信が正常完了したか否かを示す結果である第２のレポート受信結果を作成する機能も有し、前記共通秘密情報消去手段が、当該第１のレポート受信解析手段で作成された前記第２のレポート受信結果が正常を意味する場合に、前記個別秘密情報端末蓄積手段で蓄積している前記個別秘密情報を消去する機能も有し、前記共通秘密情報端末蓄積手段が、前記第１のレポート受信解析手段で取出された前記共通秘密情報を蓄積する機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５０】本発明装置の第１５の特徴は、上記本発明装置の第１３又は第１４の特徴における前記第１の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報を、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報とを用いて暗号化して第２の署名情報を作成する機能も有し、前記第１のリクエスト作成送信手段が、前記センタに対して前記共通秘密情報を含む前記第２のレポートの送信要求を行うために、前記第２の署名情報作成手段で作成された前記第２の署名情報を含むメッセージである第２のリクエストを作成し、前記センタに前記通信網を介して送信する機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５１】本発明装置の第１６の特徴は、上記本発明装置の第１５の特徴における前記第１のリクエスト受信解析手段が、前記端末から送信される前記第２のリクエストを受信し、当該第２のリクエストに含まれる前記署名情報を取出す機能も有し、第１の署名情報認証手段が、前記個別秘密情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて、前記第２のリクエスト受信解析手段で取出された前記第２の署名情報に含まれる前記端末情報を取出し、当該第２の署名情報の正当性を認証した結果である第２の認証結果を作成する機能も有し、前記個別秘密情報送信指示手段が、前記第１の署名情報認証手段で作成された前記第２の認証結果が正常の場合に、前記第１の署名情報認証手段で取出された前記端末情報に示される端末への第２のレポートの送信指示を前記第１のレポート作成送信手段に対して行う機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５２】本発明装置の第１７の特徴は、上記本発明装置の第１５又は第１６の特徴における前記第１の署名

識別子作成手段が、前記第２の署名情報を作成する度に毎回異なる値である第２の署名識別子を作成する機能も有し、前記第１の署名情報作成手段が、前記端末情報蓄積手段に蓄積された前記端末情報と、前記第２の署名識別子作成手段で作成された前記第２の署名識別子とを、前記個別秘密情報端末蓄積手段に蓄積された前記個別秘密情報を用いて暗号化をして、前記第２の署名情報を作成する機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５３】本発明装置の第１８の特徴は、上記本発明装置の第１７の特徴における前記第１の署名情報認証手段が、前記個別情報センタ蓄積手段に蓄積された前記個別秘密情報を用いて復号化をして、前記第１のリクエスト情報受信解析手段で取出された前記第２の署名情報から前記端末情報及び前記第２の署名識別子を取出し前記第２の署名情報の正当性を認証した第２の認証結果を作成する機能も有し、前記第１の署名識別子使用状況確認手段が、前記第１の署名情報認証手段で取出された前記第２の署名識別子が過去に既に使用済みか否かを示す結果である第２の確認結果を作成する第２の署名識別子使用状況確認手段を有し、前記個別秘密情報送信指示手段が、前記第１の署名情報認証手段で作成された前記第２の認証結果が正常でかつ、前記第１の署名識別子使用状況確認手段で取出された前記第２の確認結果が未使用の場合に、前記第１の署名識別子使用状況確認手段で取出された前記端末情報に示される端末への前記第２のレポートの送信指示を、前記第２のレポート作成送信手段に対して行う機能も有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５４】本発明装置の第１９の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７又は第１８の特徴における前記通信網が、ＬＡＮや、電話及びＩＳＤＮを含む公衆通信回線のうちの少なくとも１つからなる個別秘密情報共有交信システム装置の構成採用にある。

【００５５】本発明装置の第２０の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７、第１８又は第１９の特徴における前記センタが、前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信部を有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５６】本発明装置の第２１の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７、第１８又は第１９の特徴における前記センタとは別に、前記共通秘密情報及び前記個別秘密情報を共有しセキュリティ通信を行うセキュリティ通信装置を設けてなる個別秘密情報共有交信システム装置の構成採用にある。

【００５７】本発明装置の第２２の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における前記センタ及び前記各端末が、別に、前記共通秘密情報を時間関数及び設定自在なパラメータとする世代識別子の関数を入力及び蓄積する鍵注入器を設けてなる個別秘密情報共有交信システム装置の構成採用にある。

【００５８】本発明装置の第２３の特徴は、上記本発明装置の第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４、第１５、第１６、第１７、第１８、第１９、第２０、第２１又は第２２の特徴における前記第１の署名識別子作成手段が、前記第１の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの１つを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００５９】本発明装置の第２４の特徴は、上記本発明装置の第１１、第１２、第１７、第１８、第１９、第２０、第２１、第２２又は第２３の特徴における前記第２の署名識別子が、前記第２の署名情報を作成する度にカウントアップするカウンタ及び乱数を発生するプログラムのうちの１つを有してなる個別秘密情報共有交信システム装置の構成採用にある。

【００６０】

【発明の実施の形態】以下、添付図面を参照して、本発明の一実施形態に係る方法例及びこれに対応する装置例につき順に説明する。

【００６１】（装置例）本装置例を図１乃至図５を参照して説明する。図１は、本装置例の個別秘密情報共有交信システム装置を示す全体構成図であり、図２は、個別秘密情報共有交信システム装置のセンタの内部構成ブロック図であり、図３は、個別秘密情報共有交信システム装置の端末の内部構成ブロック図であり、図４は、センタと端末との間での通信を示す説明図であり、図５は、センタと端末との間及び各端末間での通信を示す説明図である。

【００６２】本装置例の個別秘密情報共有交信システム装置αは、共通秘密情報Ｐ及び個別秘密情報Ｓ１～Ｓｋ（ｋは任意の自然数）を共有するセンタ１と、センタ１から共有秘密情報Ｐ及び各個別秘密情報Ｓ１～Ｓｋを取寄せる端末２－１～２－ｋと、センタ１と各端末２－１～２－ｋとを接続しＬＡＮ又は電話、ＩＳＤＮ等の公衆通信回線等である通信網３とを有する。センタ１と端末２－１～２－ｋとの間に新しく通信回線を設ける必要はない。

【００６３】センタ１は、図４乃至図５に示すよう、個別秘密情報Ｓ１～Ｓｋを各端末２－１～２－ｋへ送信する個別秘密情報払い出し部４と、各端末２－１～２－ｋとセキュリティ通信を行うセキュリティ通信部５とを有

する。

【００６４】また、図２及び図３においては、センタ１と全端末２－１～２－ｋ中の端末２－ｋとの間の接続による端末２－ｋの構成を説明したものであり、他の端末２－１～２－（ｋ－１）についても端末２－ｋと同様の構成を採る。よって、ここでは、端末２－ｋと接続されたセンタ１及び端末２－ｋの構成を代表して説明する。

【００６５】個別秘密情報払い出し部４は、共通秘密情報Ｐを蓄積する共通秘密情報センタ蓄積手段６と、全端末２－１～２－ｋの個別秘密情報Ｓ１～Ｓｋを蓄積する個別秘密情報センタ蓄積手段７と、各端末２－１～２－ｋからの署名情報ａ１を有するリクエストｂ１を受信し署名情報ａ１を取出すリクエスト受信解析手段８と、リクエスト受信解析手段８からの署名情報ａ１から端末情報ＩＤ及び署名識別子Ｒ１を取出し認証を行い認証結果ｃ１を作成する署名情報認証手段９と、署名情報認証手段９からの署名識別子Ｒ１の使用状況から確認結果ｄ１を作成する署名識別子使用状況確認手段１０と、署名情報認証手段９からの認証結果ｃ１及び署名識別子使用状況確認手段１０からの確認結果ｄ１により個別秘密情報Ｓｋの送信指示を行う個別秘密情報送信指示手段１１と、個別秘密情報送信指示手段１１からの送信指示によりレポートｅ１を作成し各端末２－１～２－ｋへ送信するレポート作成送信手段１２とを有する。

【００６６】また他に、各端末２－１～２－ｋからの署名情報ａ２を有するリクエストｂ２を受信し署名情報ａ２を取出すリクエスト受信解析手段１３と、リクエスト受信解析手段１３からの署名情報ａ２から端末情報ＩＤ及び署名識別子Ｒ２を取出し認証を行い認証結果ｃ２を作成する署名情報認証手段１４と、署名情報認証手段１４からの署名識別子Ｒ２の使用状況から確認結果ｄ２を作成する署名識別子使用状況確認手段１５と、署名情報認証手段１４からの認証結果ｃ２及び署名識別子使用状況確認手段１５からの確認結果ｄ２により共通秘密情報Ｐの送信指示を行う共通秘密情報送信指示手段１６と、共通秘密情報送信指示手段１６からの送信指示によりレポートｅ２を作成し各端末２－１～２－ｋへ送信するレポート作成送信手段１７とを有する。

【００６７】端末２－ｋは、端末情報ＩＤを蓄積する端末情報蓄積手段１８と、署名識別子Ｒ１を作成する署名識別子作成手段１９と、共通秘密情報Ｐを蓄積する共通秘密情報蓄積手段２０と、共通秘密情報蓄積手段２０からの共通秘密情報Ｐを用いて端末情報蓄積手段１８からの端末情報ＩＤ及び署名識別子作成手段１９からの署名識別子Ｒ１から署名情報ａ１を作成する署名情報作成手段２１と、署名情報作成手段２１からの署名情報ａ１からリクエストｂ１を作成及びセンタ１へ送信するリクエスト作成送信手段２２と、センタ１からのレポートｅ１を受信し個別秘密情報Ｓｋを取出してレポート受信結果ｈ１を作成するレポート受信解析手段２３と、レポート受信解析手段２３からの個別秘密情報Ｓｋを蓄積する個別秘密情報端末蓄積手段２４と、レポート受信解析手段２３からのレポート受信結果ｈ１により共通秘密情報蓄積手段２０の共通秘密情報Ｐを消去する共通秘密情報消去手段２５とを有する。

【００６８】また他に、署名識別子Ｒ２を作成する署名識別子作成手段２６と、個別秘密情報蓄積手段２４からの個別秘密情報Ｓｋを用いて端末情報蓄積手段１８からの端末情報ＩＤ及び署名識別子作成手段２６からの署名識別子Ｒ１から署名情報ａ２を作成する署名情報作成手段２７と、署名情報作成手段２７からの署名情報ａ２からリクエストｂ２を作成及びセンタ１へ送信するリクエスト作成送信手段２８と、センタ１からのレポートｅ２を受信し共通秘密情報Ｐを取出しレポート受信結果ｈ２を作成するレポート受信解析手段２９と、レポート受信解析手段２９からのレポート受信結果ｈ２により個別秘密情報蓄積手段２４の個別秘密情報Ｓｋを消去する個別秘密情報消去手段３０とを有する。

【００６９】なお、図４は、センタ１と各端末２－１～２－ｋとの間で通信を行う場合であり、秘密情報センタ蓄積エリア３１ａは、センタ１において、共通秘密情報Ｐ及び個別情報秘密情報Ｓ１～Ｓｋを蓄積し、共通秘密情報センタ蓄積手段６及び個別秘密情報センタ蓄積部７に相当し、秘密情報端末蓄積エリア３２ａ－１～３２ａ－ｋは、各端末２－１～２－ｋにおいて、共通秘密情報Ｐ及び個別情報秘密情報Ｓ１～Ｓｋのそれぞれを蓄積し、共通秘密情報端末蓄積手段２０及び個別秘密情報端末蓄積部２４に相当する。

【００７０】また、図５は、センタ１と各端末２－１～２－ｋとの間及び各端末２－１～２－ｋ間で通信を行う場合であり、秘密情報センタ蓄積エリア３１ｂは、センタ１において、共通秘密情報Ｐ、個別情報秘密情報Ｓ１～Ｓｋ及び端末２－ｐから端末２－ｑへの秘密情報である端末間秘密情報Ｓｐ，ｑ（ｐ，ｑ＝１～ｋ、ｐ≠ｑ）を蓄積し、秘密情報蓄積エリア３２ｂ－１～３２ｂ－ｋは、例えば、端末２－ｋにおいて、共通秘密情報Ｐ及び個別情報秘密情報Ｓｋ，１～Ｓｋ，（ｋ－１）を蓄積する。なお、Ｓｐ，ｑ＝Ｓｑ，ｐとしてもよい。

【００７１】また、図４及び図５で示すように、センタ１は、一般に個別秘密情報払い出し部４とセキュリティ通信部５で構成されると考えることができるが、この二つは１つの装置である必要はなく、セキュリティ強度の高い通信回線で接続された別の装置で構成されてもよいことは言うまでもない。

【００７２】また、センタ１において、リクエスト受信解析手段１３、署名情報認証手段１４、署名識別子使用状況確認手段１５、共通秘密情報送信指示手段１６、レポート作成送信手段１７は、順にそれぞれ、リクエスト受信解析手段８、署名情報認証手段９、署名識別子使用状況確認手段１０、個別秘密情報送信指示手段１１、レ

ポート作成送信手段１２と同様の構成で実現可能であるから、それぞれ二つを時間的に切替えて共用することもできる。

【００７３】同じく、端末２－ｋにおいて、署名識別子作成手段２６、署名情報作成手段２７、リクエスト作成送信手段２８、レポート受信解析手段２９、個別秘密情報消去手段３０は、順にそれぞれ、署名識別子作成手段１９、署名情報作成手段２１、リクエスト作成送信手段２２、レポート受信解析手段２３、共通秘密情報消去手段２５と同様の構成で実現可能であるから、それぞれ二つを時間的に切替えて共用することもできる。

【００７４】（方法例）本方法例は、前記装置例に適用したものであり、同じく図１乃至図５と、他に図６及び図７を参照して説明する。図６は、本方法例のステップ１におけるリクエストｂ１の形成を示す説明図であり、図７は、本方法例のステップ４におけるリクエストｂ２の形成を示す説明図である。

【００７５】また、本方法例の手順をステップ１乃至ステップ５に分けて順に説明する。ステップ１及びステップ２は、在庫状態であった端末が運用（セキュリティ通信）を開始するために設置時等の事前に行われる。ステップ３は、運用（セキュリティ通信）を行う段階である。ステップ４及びステップ５は、運用段階にあった端末を一旦撤去し、（将来の設置のために）在庫状態にする必要がある場合等に行われるものである。以下、全端末２－１～２－ｋのうちの端末２－ｋと、センタ１との間での手順を説明するが、他の端末も同様の手順で行われる。

【００７６】なお、ステップ１，２，４，５は、センタ１の個別秘密情報払い出し部４と端末２－ｋとの間の手順であり、ステップ３は、センタ１のセキュリティ通信部５と端末２－ｋとの間の手順である。

【００７７】＜ステップ１＞ステップ１は、端末２－ｋからセンタ１へ個別秘密情報Ｓｋの受信要求（リクエストｂ１）を行う手順である。センタ１から個別秘密情報Ｓｋの送信を自発的に行い、端末２－ｋから受信要求を行う必要が無い場合には、当該ステップ１は必要無い。

【００７８】先ず、端末２－ｋにおいて、端末情報蓄積手段１８に、センタ１が全端末２－１～２－ｋの中で当該端末２－ｋを識別可能な端末情報ＩＤを蓄積する。端末情報ＩＤとしては、端末２－ｋ自身が接続されている通信回線のアドレス情報や、センタ１が割り振った連続番号等を使用することが可能であるが、各端末２－１～２－ｋで重複しないものでなくてはならない。また、端末情報ＩＤの入力方法の一具体例としては、設置時に作業者が、前記接続されている通信回線のアドレス等を入力する方法等がある。

【００７９】また、署名識別子作成手段１９によって、署名識別子Ｒ１を作成する。署名識別子Ｒ１は、署名情報作成手段２１で署名情報ａ１を作成する度に異なる値であるものであり、具体的には、署名情報作成手段２１で署名情報ａ１を作成する度にカウントアップするカウンタや、乱数を生成するプログラム等で実現することが可能である。

【００８０】また、予め共通秘密情報端末蓄積手段２０によって、及びセンタ１の共通秘密情報センタ蓄積手段６によって、共に共通の共通秘密情報Ｐを蓄積する。共通秘密情報Ｐは、予めセンタ１と全端末２－１～２－ｋとの間で共有しておかなければならないが、共通秘密情報Ｐは全端末２－１～２－ｋで共通な情報であることから、端末２－ｋの製造段階でセンタ１が指定した情報を全端末２－１～２－ｋの不揮発性メモリ等の情報蓄積媒体に予め書き込んでおくことで容易に実現可能である。

【００８１】そして、署名情報作成手段２１によって、端末情報蓄積手段１８に蓄積された端末情報ＩＤと署名識別子作成手段１９で作成された署名識別子Ｒ１とを、共通秘密情報端末蓄積手段２０からの共通秘密情報Ｐを用いて、センタ１に送信する署名情報ａ１を作成する。

【００８２】署名情報ａ１の作成処理の一具体例としては、図６に示すように予め指定された暗号化関数ｆを用いて、端末情報ＩＤと署名識別子Ｒ１を、共通秘密情報Ｐを暗号鍵として暗号化したデータf_P（ＩＤ，Ｒ１）を、端末情報ＩＤ及び署名識別子Ｒ１と一緒に送信する方法が考えられる。

【００８３】署名情報ａ１の作成処理では、暗号化関数ｆの入力値と出力値が通信網３上に現れることから、通信網３上のモニタ信号から共通秘密情報Ｐを推測することが事実上不可能とするためには、暗号化関数ｆに、暗号化した情報と元の情報から暗号を求める既知平文攻撃への十分な耐性を有するものを用いることが望ましい。また、ここでは暗号鍵を共通秘密情報Ｐとして説明したが、実際には暗号化関数ｆと暗号鍵の組合せ自体が暗号鍵と考えることもできる。

【００８４】上記のように、端末情報ＩＤと署名識別子Ｒ１を組合せたものを、共通秘密情報Ｐで処理したものを署名情報ａ１として用いることにより、センタ１が受信するリクエストｂ１に含まれる署名情報ａ１として、同一内容のリクエストｂ１が２回以上使用されないことが保障される。よって、不正者が、過去に使用されたリクエストｂ１を通信網３上でモニタしたものを、不正アクセス時に送信する信号としてそのまま用いたとしても、センタ１ではこれを検出し排除することが可能となる。

【００８５】そして、リクエスト作成送信手段２２によって、署名情報ａ１を含むリクエストｂ１を作成し、通信網３を介してセンタ１に送信する。通信網３の公衆通信回線を用いる場合のリクエストｂ１の送信の具体的な動作としては、先ず発呼動作を行いセンタ１との回線接続が完了した後、確保された通信チャネル上でリクエストｂ１メッセージの送信を行うこととなる。

【００８６】次に、センタ１において、リクエスト受信解析手段８では、端末２－ｋのリクエスト作成送信手段２２から通信回線を介して送信されたリクエストｂ１を受信して、含まれる署名情報ａ１を取出す。

【００８７】そして、署名情報認証手段９によって、共通秘密情報センタ蓄積手段６に蓄積された共通秘密情報Ｐを用いて、リクエスト受信解析手段８で取出された署名情報ａ１に含まれる端末情報ＩＤ及び署名識別子Ｒ１を取出すとともに、署名情報ａ１の正当性を認証した結果である認証結果ｃ１を作成する。

【００８８】この署名情報ａ１からの認証処理の一具体例を以下に示す。ここで示す例は、上記に記載した、署名情報ａ１として図６に示すように予め指定された暗号化関数ｆを用いて端末情報ＩＤと署名識別子Ｒ１を、共通秘密情報Ｐを暗号鍵として暗号化したものを、端末情報ＩＤと署名識別子Ｒ１とを一緒に送信する場合に対応するものである。

【００８９】署名情報認証手段９では、リクエスト受信解析手段８で取出された署名情報ａ１に含まれる暗号化データf_P（ＩＤ，Ｒ１）を、暗号化関数ｆと共通秘密情報センタ蓄積手段６に蓄積された共通秘密情報Ｐである暗号鍵を用いて復号化して得られた復号化端末情報ＩＤ′と復号化署名識別子Ｒ１′を、署名情報ａ１に含まれる端末情報ＩＤ及び署名識別子Ｒ１とそれぞれ比較し、一致するか否かをチェックする。当該チェックを行った結果、両者が一致した場合には、端末２－ｋが正規の共通秘密情報Ｐを具備しているものと判断できることから、認証結果ｃ１を正常とする。

【００９０】そして、署名識別子使用状況確認手段１０によって、署名情報認証手段９で取出された端末情報ＩＤに示される各端末毎に、過去に既に使用された署名識別子Ｒ１を管理し、署名情報認証手段９で取出された署名識別子Ｒ１が未使用か否かをチェックし、確認結果ｄ１として作成する。

【００９１】＜ステップ２＞ステップ２は、センタ１から端末２－ｋに対して個別秘密情報Ｓｋの送信を行う手順である。ステップ２は、本方法例において、必須の手順である。

【００９２】先ず、センタ１において、個別秘密情報送信指示手段１１によって、署名情報認証手段９で作成された認証結果ｃ１が正常でかつ、署名識別子使用状況確認手段１０で作成された確認結果ｄ１が未使用の場合に、署名情報認証手段９で取出された端末情報ＩＤに示される端末２－ｋへのレポートｅ１の送信指示をレポート作成送信手段１２に対して行う。

【００９３】また、予め個別秘密情報センタ蓄積手段７によって、各端末毎の個別秘密情報Ｓｋを蓄積する。個別秘密情報センタ蓄積手段７では、全端末２－１～２－ｋの分の個別秘密情報Ｓ１～Ｓｋを蓄積し、また個別秘密情報Ｓｋとして予め作成しておいたものを蓄積しても良いし、必要に応じて作成して蓄積してもよいが、一旦端末２－１～２－ｋに送信済のものについては蓄積しておく必要がある。

【００９４】個別秘密情報Ｓｋ及び共通秘密情報Ｐとしては、データの暗号化を行う場合には暗号鍵、認証を行う場合にはユーザ名やパスワード等を含むし、セキュリティ通信時に使用する通信回線やポートを特定する場合にはこれらの情報を含むこととなる。

【００９５】そして、レポート作成送信手段１２によって、個別秘密情報送信指示手段１１からのレポートｅ１の送信指示に従い、個別秘密情報センタ蓄積手段７に蓄積された個別秘密情報Ｓｋを、共通秘密情報センタ蓄積手段６に蓄積された共通秘密情報Ｐで暗号化した暗号化個別秘密情報Ｓｋ′を含むメッセージであるレポートｅ１を作成し、端末２－ｋに通信網３を介して送信する。

【００９６】次に、端末２－ｋにおいて、レポート受信解析手段２３によって、センタ１のレポート作成送信手段１２から送信されるレポートｅ１を受信し、レポートｅ１に含まれる暗号化個別秘密情報Ｓｋ′を、共通秘密情報端末蓄積手段２０に蓄積された共通秘密情報Ｐで復号化し個別秘密情報Ｓｋを取出すとともに、個別秘密情報Ｓｋの受信が正常完了したか否かを示す結果であるレポート受信結果ｈ１を作成する。

【００９７】そして、個別秘密情報端末蓄積手段２４によって、レポート受信解析手段２３により取出された個別秘密情報Ｓｋを蓄積する。

【００９８】そして、共通秘密情報消去手段２５によって、レポート受信解析手段２３で作成されたレポート受信結果ｈ１が正常を意味する場合に、第三者が端末２－ｋから共通秘密情報Ｐを取出さないように、共通秘密情報端末蓄積手段２０で蓄積している共通秘密情報Ｐを消去する。

【００９９】＜ステップ３＞ステップ３は、端末２－ｋとセンタ１との間で個別秘密情報Ｓｋを用いてセキュリティ通信を行う手順である。具体的には個別秘密情報Ｓｋを暗号鍵として用いたり、認証に用いる以外にも実際に通信を行う際に用いるアドレスやポートを指定する情報として用いることもできる。

【０１００】また、本方法例において、図４に示すようにセンタ１のセキュリティ通信部５と端末２－ｋとの間で通信網３を介してセキュリティ通信を行う際に用いる個別秘密情報Ｓ１～Ｓｋのみを共有する例を記述しているが、図５に示すようにセンタ１と端末２－ｋとの間だけでなく端末相互２－１～２－ｋ間でセキュリティ通信を行うために用いる秘密情報である端末間秘密情報を個別秘密情報Ｓ１～Ｓｋに含めることも可能であることは言うまでもない。

【０１０１】この場合には、センタ１から端末２－ｋに送信されるレポートに含まれる個別秘密情報として、センタ１と端末２－ｋとの間の個別秘密情報Ｓｋ以外に

も、端末２－ｋから他の全端末への端末間秘密情報Ｓｋ，ｑ（ｑ＝１～全端末数ｋ：但しｋを除く）を含めておけばよい。

【０１０２】＜ステップ４＞ステップ４は、端末２－ｋからセンタ１へ共通秘密情報Ｐの受信要求（リクエストｂ１）を行う手順である。センタ１から共通秘密情報Ｐの送信を自発的に行い、端末２－ｋから受信要求を行う必要が無い場合にはステップ４は必要無く、また、端末２－ｋで共通秘密情報Ｐの再構築が必要ない場合にもステップ４は必要無い。

【０１０３】先ず、端末２－ｋにおいて、署名識別子作成手段２６によって、署名識別子Ｒ２を作成する。署名識別子Ｒ２は、署名情報作成手段２７で署名情報ａ２を作成する度に異なる値であるものであり、具体的には、署名情報作成手段２７で署名情報ａ２を作成する度にカウントアップするカウンタや、乱数を生成するプログラム等で実現することが可能である。

【０１０４】そして、署名情報作成手段２７によって、端末情報蓄積手段１８に蓄積された端末情報ＩＤと署名識別子作成手段２６で作成された署名識別子Ｒ２とを、個別秘密情報端末蓄積手段２４からの個別秘密情報Ｓｋを用いて、センタ１に送信する署名情報ａ２を作成する。

【０１０５】署名情報ａ２の作成処理の一具体例としては、図７に示すように予め指定された暗号化関数ｇを用いて、端末情報ＩＤと署名識別子Ｒ２を、個別秘密情報Ｓｋを暗号鍵として暗号化したデータg_{Sk}（ＩＤ，Ｒ２）を、端末情報ＩＤ及び署名識別子Ｒ２と一緒に送信する方法が考えられる。

【０１０６】当該署名情報ａ２の作成処理では、暗号化関数ｇの入力値と出力値が通信網３上に現れることから、通信網３上のモニタ信号から個別秘密情報Ｓｋを推測することが事実上不可能とするためには、暗号化関数ｇに既知平文攻撃への十分な耐性を有するものを用いることが望ましい。また、ここでは暗号鍵を個別秘密情報Ｓｋとして説明したが、実際には暗号化関数ｇと暗号鍵の組合せ自体が暗号鍵と考えることもできる。

【０１０７】上記のように、端末情報ＩＤと署名識別子Ｒ２を組合せたものを、個別秘密情報Ｓｋで処理したものを署名情報ａ２として用いることにより、センタ１が受信するリクエストｂ２に含まれる署名情報ａ２として、同一内容のリクエストｂ２が２回以上使用されないことが保障される。よって、不正者が、過去に使用されたリクエストｂ２を通信網３上でモニタしたものを、不正アクセス時に送信する信号としてそのまま用いたとしても、センタ１ではこれを検出し排除することが可能となる。

【０１０８】そして、リクエスト作成送信手段２８によって、署名情報ａ２を含むリクエストｂ２を作成し、通信網３を介してセンタ１に送信する。

【０１０９】次に、センタ１において、リクエスト受信解析手段１３では、端末２－ｋのリクエスト作成送信手段２８から通信網３を介して送信されたリクエストｂ２を受信して、含まれる署名情報ａ２を取出す。

【０１１０】そして、署名情報認証手段１４によって、個別秘密情報センタ蓄積手段７に蓄積された個別秘密情報Ｓｋを用いて、リクエスト受信解析手段１３で取出された署名情報ａ２に含まれる端末情報ＩＤ及び署名識別子Ｒ２を取出すとともに、署名情報ａ２の正当性を認証した結果である認証結果ｃ２を作成する。

【０１１１】この署名情報ａ２の認証処理の一具体例を以下に示す。ここで示す例は、上記に記載した、署名情報ａ２として図７に示すように予め指定された暗号化関数ｇを用いて端末情報ＩＤと署名識別子Ｒ２を、個別秘密情報Ｓｋを暗号鍵として暗号化したものを、端末情報ＩＤと署名識別子Ｒ２とを一緒に送信する場合に対応するものである。

【０１１２】署名情報認証手段１４では、リクエスト受信解析手段１３で取出された署名情報ａ２に含まれる暗号化データg_{Sk}（ＩＤ，Ｒ２）を、暗号化関数ｇと個別秘密情報センタ蓄積手段７に蓄積された個別秘密情報Ｓｋである暗号鍵を用いて復号化して得られた復号化端末情報ＩＤ″と復号化署名識別子Ｒ２′を、署名情報ａ２に含まれる端末情報ＩＤ及び署名識別子Ｒ２とそれぞれ比較し、一致するか否かをチェックする。当該チェックを行った結果、両者が一致した場合には、端末２－ｋが正規の個別秘密情報Ｓｋを具備しているものと判断できることから、認証結果ｃ２を正常とする。

【０１１３】そして、署名識別子使用状況確認手段１５によって、署名情報認証手段１４で取出された端末情報ＩＤに示される各端末毎に、過去に既に使用された署名識別子Ｒ２を管理し、署名情報認証手段９で取出された署名識別子Ｒ２が未使用か否かをチェックし、確認結果ｄ２として作成する。

【０１１４】＜ステップ５＞ステップ５は、センタ１から端末２－ｋに対して共通秘密情報Ｐの送信を行う手順である。本方法例において、端末２－ｋで共通秘密情報Ｐの再構築が必要ない場合は、ステップ５は必要無い。

【０１１５】先ず、センタ１において、共通秘密情報送信指示手段１６によって、署名情報認証手段１４で作成された認証結果ｃ２が正常でかつ、署名識別子使用状況確認手段１５で作成された確認結果ｄ２が未使用の場合に、署名情報認証手段１４で取出された端末情報ＩＤに示される端末２－ｋへのレポートｅ２の送信指示をレポート作成送信手段１７に対して行う。

【０１１６】そして、レポート作成送信手段１７によって、共通秘密情報送信指示手段１６からのレポートｅ２の送信指示に従い、共通秘密情報センタ蓄積手段６に蓄積された共通秘密情報Ｐを、個別秘密情報センタ蓄積手段７に蓄積された個別秘密情報Ｓｋで暗号化した暗号化

共通秘密情報P′を含むメッセージであるレポートｅ２を作成し、端末２－ｋへ通信網３を介して送信する。

【０１１７】次に、端末２－ｋにおいて、レポート受信解析手段２９によって、センタ１のレポート作成送信手段１７から送信されるレポートｅ２を受信し、レポートｅ２に含まれる暗号化共通秘密情報P′を、個別秘密情報端末蓄積手段２４に蓄積された個別秘密情報Ｓｋで復号化し共通秘密情報Ｐを取出すとともに、共通秘密情報Ｐの受信が正常完了したか否かを示す結果であるレポート受信結果ｈ２を作成する。

【０１１８】そして、個別秘密情報消去手段３０によって、レポート受信解析手段２９で作成されたレポート受信結果ｈ２が正常を意味する場合に、第三者が端末２－ｋから個別秘密情報Ｓｋを取出さないように、個別秘密情報端末蓄積手段２４で蓄積している個別秘密情報Ｓｋを消去する。

【０１１９】以上述べてきた手順では、共通秘密情報Ｐは固定のものとして記述したが、万一何らかの原因で漏洩した場合にシステム全体のセキュリティ機能が停止することを考慮すると、これを防止するために予め容易に変更可能とすることが望ましい。

【０１２０】更新機能を具備する方法の一例としては、共通秘密情報Ｐを定数ではなく、時刻や日時等による時間関数とする方法が考えられる。具体的には、センタ１や端末２－ｋでは予め同期された時計機能を具備し、時計から通知される時間が随時変更されることにより、共通秘密情報Ｐは時間経過とともに自動的に変更することが可能となり、セキュリティ耐力は大幅に向上する。

【０１２１】しかし当該方法を用いた場合でも、共通秘密情報Ｐが時間関数である仕様そのものが漏洩した場合には、システム全体としてのセキュリティ機能が停止することになる。

【０１２２】これを解決する別の方法として、共通秘密情報Ｐをセンタ１及び各端末２－１～２－ｋにて何らかの形で入力可能な世代情報である世代識別子の関数とする方法が考えられる。当該世代識別子の入力方法としては、新たに端末を設置する段階で人手を介して入力する方法や、センタ１から予め通知しておく方法等が考えられる。この方法を用いることにより、万一ある世代の共通秘密情報Ｐが漏洩した場合にも、少なくとも新たな世代識別子に変更された端末については、セキュリティ機能を有効にすることができる。

【０１２３】また、前記世代識別子の関数を各端末２－１～２－ｋの内部に持たせるのではなく、各端末２－１～２－ｋのとは別の装置である鍵注入器に具備させ、人が世代情報を鍵注入器に入力し、その結果得られた出力値を各端末２－１～２－ｋに入力する方法を用いることにより、端末が盗難され内部解析されたような場合でも、波及効果を小さくすることができる。

【０１２４】以上、本発明の実施の形態につき説明したが、本発明は、必ずしも上述した手段及び手法にのみ限定されるものではなく、本発明にいう目的を達成し、本発明にいう効果を有する範囲内において、適宜に変更実施することが可能なものである。

【０１２５】

【発明の効果】以上説明したように、本発明によれば、新しく通信回線を設置することなく、センタと各端末間で経済的に安価でかつ安全に個別秘密情報を共有することができ、また、共通秘密情報を変更可能なものにすれば、万一共通秘密情報が漏洩した場合にもシステム全体に影響が及ぶことがなくなる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る個別秘密情報共有交信システム装置を示す全体構成図である。

【図２】同上、個別秘密情報共有交信システム装置のセンタの内部構成ブロック図である。

【図３】同上、個別秘密情報共有交信システム装置の端末の内部構成ブロック図である。

【図４】同上、センタと端末との間での通信を示す説明図である。

【図５】同上、センタと端末との間及び各端末間での通信を示す説明図である。

【図６】第１のリクエストの形成を示す説明図である。

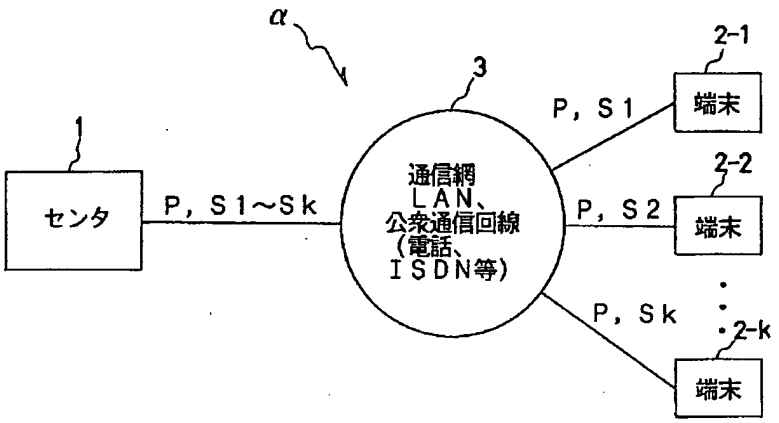
【図７】第２のリクエストの形成を示す説明図である。

【符号の説明】

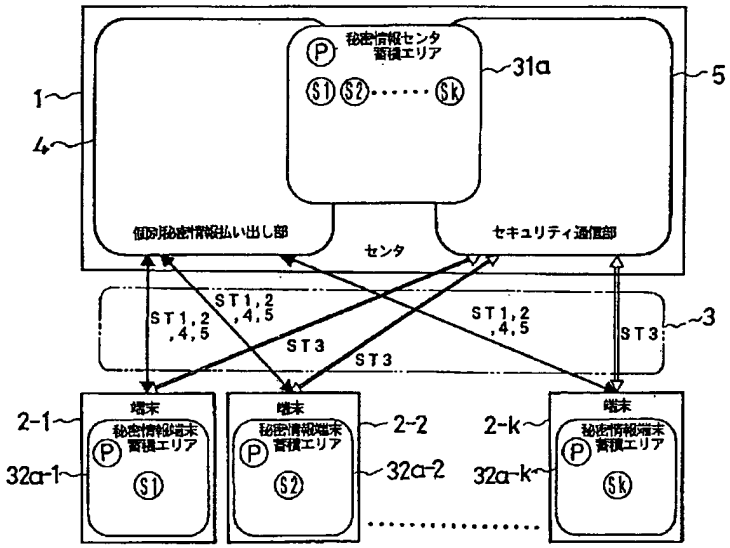
α…個別秘密情報共有交信システム装置
１…センタ
２－１～２－ｋ…端末（ｋ：任意の自然数）
３…通信網
４…個別秘密情報払い出し部
５…セキュリティ通信部
６…共通秘密情報センタ蓄積手段
７…個別秘密情報センタ蓄積手段
８，１３…リクエスト受信解析手段
９，１４…署名情報認証手段
１０，１５…署名識別子使用状況確認手段
１１…個別秘密情報送信指示手段
１２，１７…レポート作成送信手段
１６…共通秘密情報送信指示手段
１８…端末情報蓄積手段
１９，２６…署名識別子作成手段
２０…共通秘密情報端末蓄積手段
２１，２７…署名情報作成手段
２２，２８…リクエスト作成送信手段
２３，２９…レポート受信解析手段
２４…個別秘密情報端末蓄積手段
２５…共通秘密情報消去手段
３０…個別秘密情報消去手段
３１ａ，３１ｂ…秘密情報センタ蓄積エリア
３２ａ－１～３２ａ－ｋ，３２ｂ－１～３２ｂ－ｋ…秘

密情報端末蓄積エリア
ＩＤ…端末情報
Ｒ１，Ｒ２…署名識別子
Ｐ…共通秘密情報
Ｓ１～Ｓｋ…個別秘密情報
ｆ，ｇ…暗号化関数
ａ１，ａ２…署名情報
ｂ１，ｂ２…リクエスト
ｃ１，ｃ２…認証結果
ｄ１，ｄ２…確認結果
ｅ１，ｅ２…レポート
ｈ１，ｈ２…レポート受信結果
Ｓｐ，ｑ…端末間秘密情報

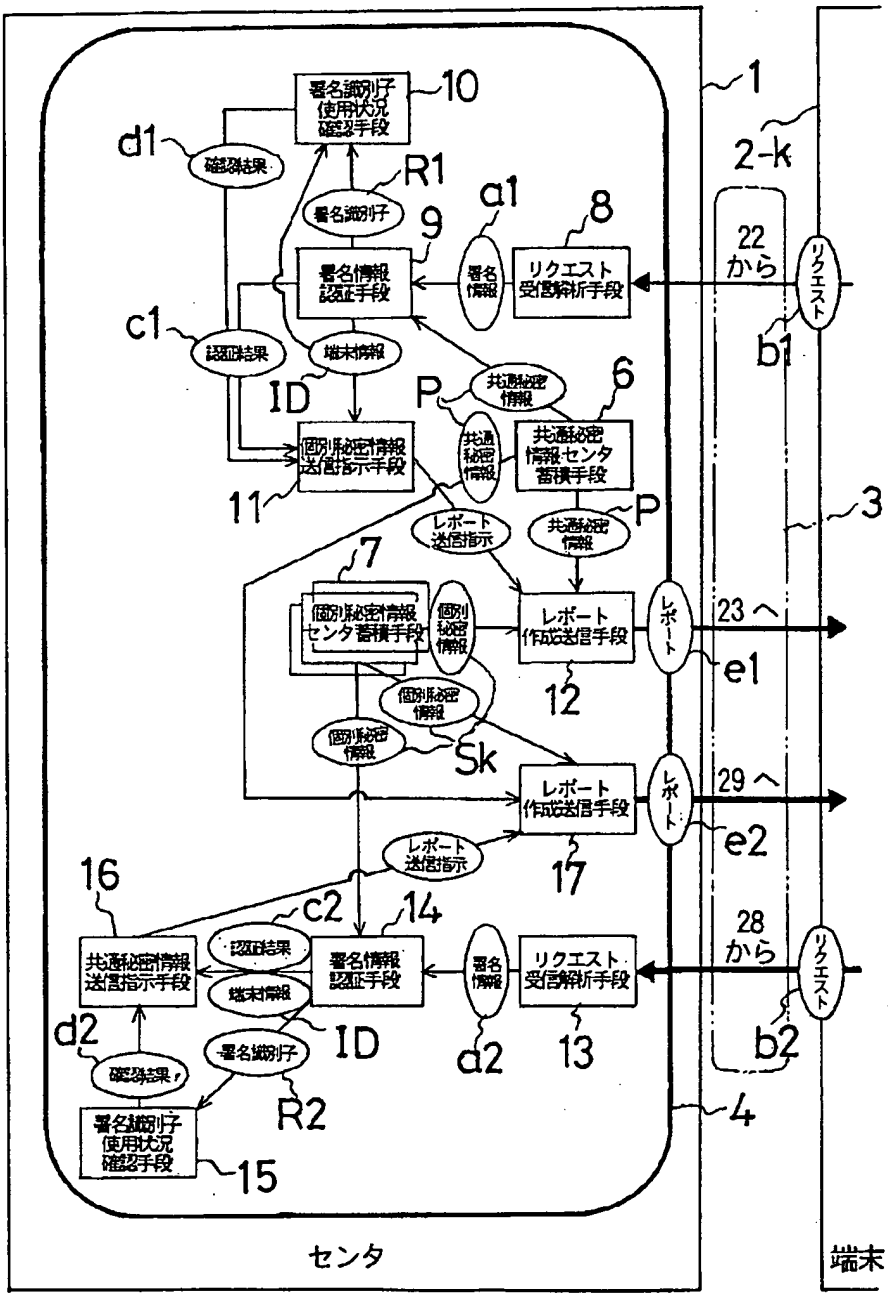
【図１】



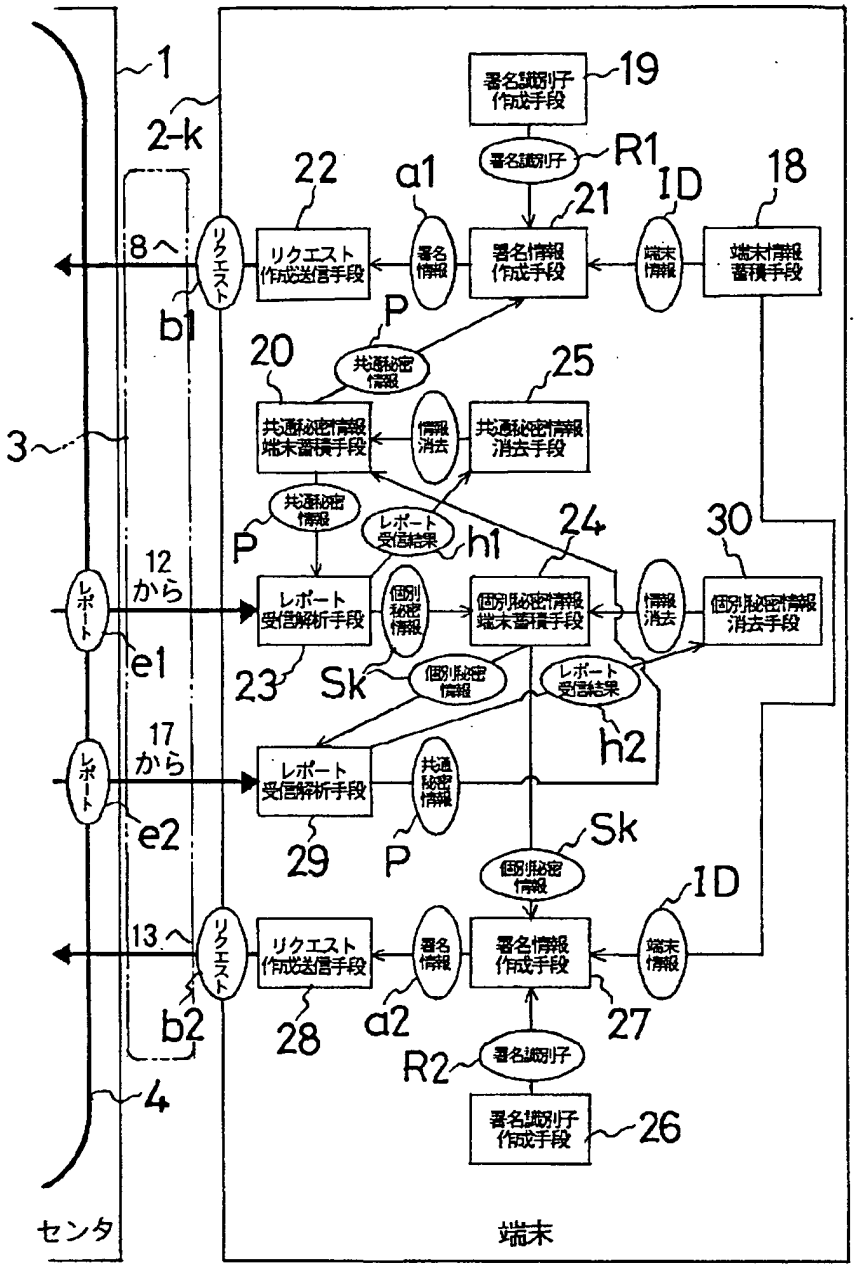
【図４】



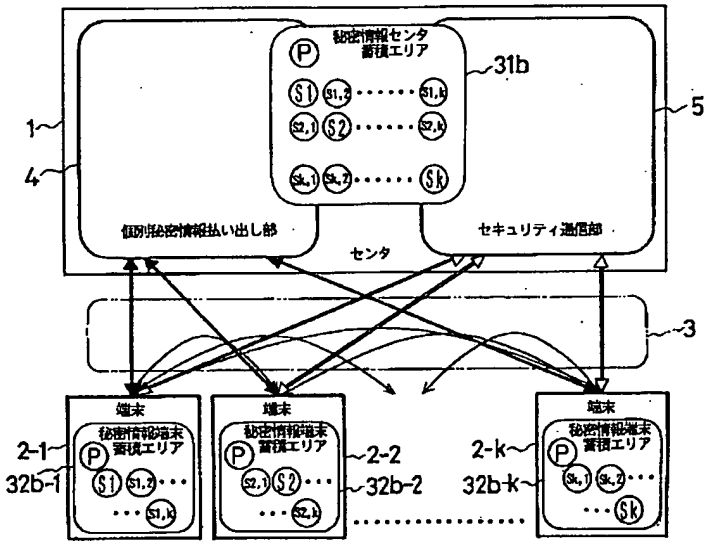
【図2】


署名識別子使用状況確認手段
10
d1
確認結果
R1
署名識別子
9
a1
8
署名情報認証手段
署名情報
リクエスト受信解析手段
22から
リクエスト
1
2-k
c1
認証結果
端末情報
ID
P
共通秘密情報
6
個別秘密情報送信指示手段
共通秘密情報
共通秘密情報センタ蓄積手段
11
レポート送信指示
P
3
7
個別秘密情報センタ蓄積手段
個別秘密情報
レポート作成送信手段
レポート
23へ
e1
12
Sk
29へ
e2
17
16
c2
14
共通秘密情報送信指示手段
28から
d2
13
b1
b2
R2
15
4
センタ
端末

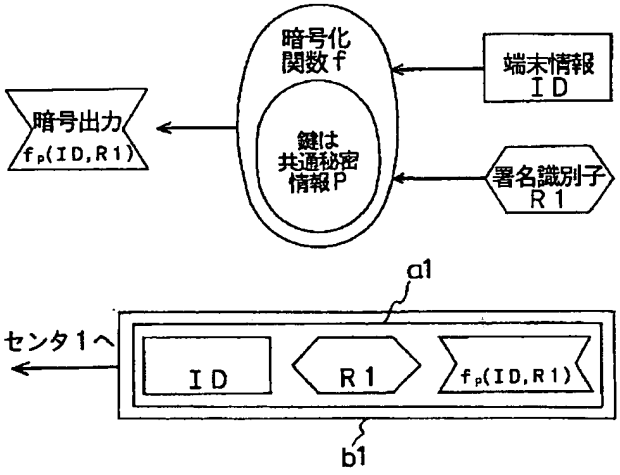
【図3】


1
2-k
署名識別子作成手段
19
署名識別子
R1
ID
18
22
a1
21
8へ
リクエスト作成送信手段
署名情報
署名情報作成手段
端末情報
端末情報蓄積手段
b1
P
共通秘密情報
20
25
3
共通秘密情報端末蓄積手段
情報消去
共通秘密情報消去手段
共通秘密情報
P
レポート受信結果
h1
24
30
12から
レポート
レポート受信解析手段
個別秘密情報
個別秘密情報端末蓄積手段
情報消去
個別秘密情報消去手段
e1
23
Sk
個別秘密情報
レポート受信結果
h2
17から
レポート
レポート受信解析手段
共通秘密情報
e2
29
P
Sk
個別秘密情報
ID
13へ
リクエスト作成送信手段
署名情報
署名情報作成手段
端末情報
b2
28
a2
27
R2
署名識別子
署名識別子作成手段
26
4
センタ
端末

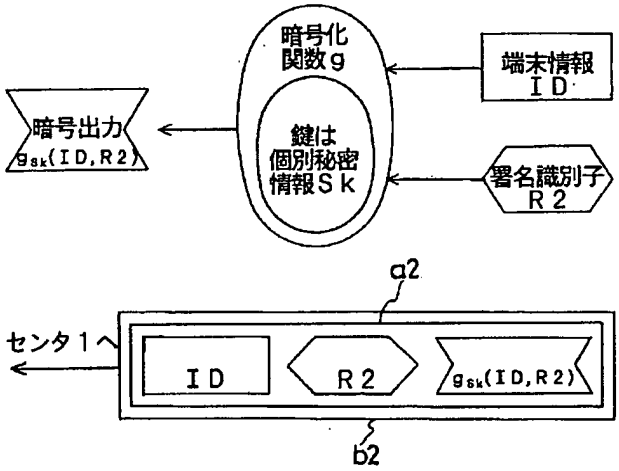
【図5】


秘密情報センタ
蓄積エリア
31b
1
4
5
個別秘密情報払い出し部
センタ
セキュリティ通信部
3
端末
秘密情報端末
蓄積エリア
2-1
32b-1
2-2
32b-2
2-k
32b-k

【図6】


暗号化
関数f
端末情報
ID
暗号出力
fp(ID,R1)
鍵は
共通秘密
情報P
署名識別子
R1
a1
センタ1へ
ID
R1
fp(ID,R1)
b1

【図7】



フロントページの続き

(72)発明者　斉藤　隆一
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　中濱　清志
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　安永　健治
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

Fターム(参考)　5K013 AA01 BA02 EA02 FA06